(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 756 074**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 13951**

(51) Int Cl[6] : **G 06 F 17/60**, G 06 F 151/00, G 07 F 7/10

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 15.11.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 22.05.98 Bulletin 98/21.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *ADVANCED PC TECHNOLOGIES APCT SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** TRUONG ANDRE, FERRY JEAN CHRISTOPHE et MICHEL GILLES.

(73) **Titulaire(s) :** .

(74) **Mandataire :** CABINET ORES.

(54) PROCEDE DE SECURISATION ET DE CONTROLE D'ACCES A DES INFORMATIONS A PARTIR D'UNE PLATE-FORME INFORMATIQUE EQUIPEE D'UN MICRO-ORDINATEUR.

(57) Procédé de sécurisation et de contrôle d'accès à des informations à partir d'une plate-forme informatique équipée d'un micro-ordinateur, caractérisé en ce qu'il consiste:

- à produire au moins un support d'enregistrement non réinscriptible sur lequel sont stockées des informations telles que des données et/ou applications selon un format logique prédéterminé, ainsi qu'un logiciel d'exploitation de ces informations,
- à configurer ou transformer la plate-forme informatique d'un utilisateur autorisé en un poste de travail sécurisé pour interdire toute intrusion matérielle et/ou logicielle visant à accéder indûment aux informations ou à en faire usage en lieu et place d'un utilisateur autorisé et sans son accord, et
- à charger le logiciel d'exploitation à partir du support d'enregistrement qui est lu par un dispositif de lecture approprié de la plate-forme informatique.

FR 2 756 074 - A1

2756074

PROCÉDÉ DE SÉCURISATION ET DE CONTRÔLE D'ACCÈS A DES INFORMATIONS A PARTIR D'UNE PLATE-FORME INFORMATIQUE ÉQUIPÉE D'UN MICRO-ORDINATEUR

La présente invention concerne un procédé de sécurisation et de contrôle d'accès à des informations telles que des données et/ou des applications, à partir d'une plate-forme informatique équipée d'un micro-ordinateur.

D'une manière générale, le fort développement du marché des micro-ordinateurs, de la technologie des réseaux et des supports d'enregistrement de forte capacité et peu onéreux, crée des conditions favorables pour développer notamment la communication et/ou l'échange d'informations, ainsi que des activités commerciales fondées sur la mise à disposition, à la demande et sous forme payante, à des utilisateurs potentiels de données et/ou d'applications à partir de plates-formes informatiques équipées d'un micro-ordinateur, en particulier du type personnel.

Or, par définition, un micro-ordinateur personnel est une machine informatique qui est conçue pour un usage pluraliste (applications personnelles ou professionnelles, ludiques ou techniques,...), c'est-à-dire une machine informatique qui présente une architecture dite « ouverte », en ce sens que de nouveaux éléments tant logiciels que matériels peuvent être aisément ajoutés pour modifier la configuration de la machine en fonction des besoins propres des utilisateurs et/ou des services ou applications auxquels les utilisateurs peuvent accéder gratuitement ou non.

Il en résulte des plates-formes informatiques qui évoluent dans un contexte globalement non sécurisé et qui est d'autant moins sécurisé que cette évolution s'accompagne toujours, en parallèle, de la mise au point de techniques de piratage. Cette évolution parallèle du piratage n'est pas sans poser des problèmes en fonction des utilisations, services et/ou applications qui peuvent être mis en oeuvre à partir de ces plates-formes informatiques à architecture dite « ouverte ».

Pour résoudre ces problèmes, de nombreuses solutions ont été proposées dans le domaine de la sécurité, comme par exemple :

- la mise en place de codes d'identification pour identifier au préalable les utilisateurs avant toute communication ou échange de données,

- la mise en place de codes d'accès pour obtenir l'autorisation d'accéder à des données et/ou à des applications,

- le recours aux techniques d'encodage/ d'encryptage pour garantir la confidentialité ou le secret des données transmises ou échangées, et/ou

- des certificats pour authentifier l'origine et l'exactitude des données transmises ou échangées, ...

Or, ces solutions même avec un degré élevé de sophistication, s'avèrent insuffisantes et, pour s'en convaincre, il suffit de donner l'exemple particulier concernant le développement des activités commerciales qui, comme cela a été évoqué précédemment, sont fondées sur la mise à disposition d'informations, à la demande et sous forme payante. En effet, même avec tout ou partie

des solutions proposées précédemment, ces applications ne peuvent être viables si l'accès aux informations se fait à partir d'une plate-forme informatique non sécurisée.

En effet, la fiabilité des contrôles de sécurité qui permettent de garantir qu'un utilisateur est bien habilité à accéder à ces informations et/ou que les droits correspondant à cet accès ont bien été acquittés, par exemple, ne pourra jamais être garantie dès l'instant où ces contrôles sont effectués dans un environnement non sécurisé.

Or, le but de l'invention est justement de proposer un procédé qui permette de sécuriser une plate-forme informatique, en particulier lors de l'accès à des informations telles que des données et/ou applications à partir de ces plates-formes informatiques.

A cet effet, l'invention propose un procédé de sécurisation et de contrôle d'accès à des informations à partir d'une plate-forme informatique équipée d'un micro-ordinateur, caractérisé en ce qu'il consiste :

- à produire au moins un support d'enregistrement non réinscriptible sur lequel sont stockées des informations telles que des données et/ou applications selon un format logique prédéterminé, ainsi qu'un logiciel d'exploitation de ces informations,
- à définir les utilisateurs autorisés ayant un droit d'accès aux informations stockées sur ce support d'enregistrement et les limites éventuelles de ce droit d'accès,
- à configurer ou transformer la plate-forme informatique d'un utilisateur autorisé en un poste de

travail sécurisé pour interdire toute intrusion matérielle et/ou logicielle visant à accéder indûment aux informations ou à en faire usage en lieu et place d'un utilisateur autorisé et sans son accord,

- à charger le logiciel d'exploitation à partir du support d'enregistrement qui est lu par un dispositif de lecture approprié de la plate-forme informatique,

- à permettre l'exploitation des informations stockées sur le support d'enregistrement dans les limites du droit acquis par l'utilisateur autorisé, et

- au cours de cette exploitation à échanger et/ou communiquer, de façon sécurisée, des données avec un réseau auquel la plate-forme informatique est reliée.

Le procédé définit une procédure générique qui permet de sécuriser une plate-forme informatique de type micro-ordinateur personnel en réseau, par exemple, de manière à permettre l'accès et l'exploitation en toute sécurité de données et d'applications par les seuls utilisateurs en ayant le droit et ce, dans les limites de ce droit.

Un tel procédé n'impose pas de normes physiques (format physique de supports ou de données) mais définit les éléments fondamentaux d'une architecture matérielle et logicielle permettant d'exploiter en toute sécurité des données protégées par un format logique spécifique.

Cette architecture est caractérisée notamment par :

- l'amorçage du système d'exploitation depuis un support non réinscriptible,

- des standards de sécurisation de données et de communication mettant en oeuvre des algorithmes de cryptographie, des protocoles de communication sécurisés, et

- des composants matériels chargés d'exécuter des fonctions sécurisées.

La sécurité offerte par un tel procédé est de haut niveau pour un surcoût réduit d'architecture matérielle et logicielle.

En effet, le coût des composants matériels à ajouter à une architecture d'un micro-ordinateur personnel de base ou de référence est modeste, les composants utilisés sont standards et peuvent être ajoutés de manière incrémentale à cette architecture de base, et le coût du logiciel est fixe pour chaque système d'exploitation supporté, indépendamment des données et des applications devant être protégées.

D'une manière générale, le procédé peut être mis en oeuvre sur deux types de plates-formes informatiques :

- une plate-forme fermée qui a été conçue initialement pour intégrer les éléments matériels de sécurisation au niveau de l'architecture matérielle de base (au niveau de la carte mère), et

- une plate-forme ouverte où une carte additionnelle a été adjointe pour apporter les composants matériels et logiciels nécessaires et suffisants pour assurer la mise en oeuvre du procédé.

Ainsi, selon un avantage important de l'invention, tout support d'enregistrement même dupliqué ne pourra être exploité sur une machine non conforme au procédé.

Selon un autre avantage, lorsque la plate-forme informatique sécurisée dialogue par le réseau avec un serveur de contrôle ou avec une autre plate-forme informatique, ce dernier est assuré que ce dialogue va se dérouler en toute sécurité.

Selon encore un autre avantage de l'invention, tout éditeur d'applications aura la garantie que les accès et les exploitations des supports d'enregistrement qu'il édite seront bien réalisés conformément aux conditions imposées aux utilisateurs.

Le procédé selon l'invention permet de sécuriser et de contrôler l'accès à des informations, ce procédé comprenant globalement trois phases principales.

La première phase concerne la production d'au moins un support d'enregistrement non réinscriptible, c'est-à-dire dont le contenu ne peut être que lu sans la possibilité de pouvoir modifier ou altérer ce contenu, sur lequel sont stockées les informations à protéger que l'on désire mettre à la disposition d'utilisateurs potentiels, généralement sous forme payante, à partir de plates-formes informatiques équipées d'un micro-ordinateur du type personnel, par exemple.

Dans cette première phase, on définit donc les informations à protéger telles que des données et/ou applications, le système d'exploitation de ces

informations et un ensemble de paramètres de contrôle et de sécurité.

Les paramètres de contrôle sont nécessaires pour permettre le fonctionnement du logiciel d'exploitation des données et/ou applications sur les plates-formes informatiques des utilisateurs, alors que les paramètres de sécurité sont nécessaires pour sécuriser l'utilisation du support d'enregistrement d'une part, et l'exploitation des informations stockées sur ce support d'enregistrement d'autre part.

Les paramètres de sécurité pour sécuriser l'utilisation d'un support d'enregistrement sont par exemple et à titre non limitatif :

- un paramètre d'identification propre au procédé,

- un paramètre d'authentification du contenu du support d'enregistrement, comme par exemple une signature cryptée qui est calculée à partir de certaines informations stockées sur le support d'enregistrement, et

- une table de sécurisation contenant des algorithmes de décodage sous forme cryptée.

Les paramètres de sécurité pour sécuriser l'exploitation des informations stockées sur le support d'enregistrement sont par exemple et à titre non limitatif :

- un paramètre concernant un niveau de sécurité requis pour pouvoir exploiter le support d'enregistrement, et

- un paramètre d'identification propre aux données et/ou applications stockées sur le support d'enregistrement.

Toutes ces informations sont ensuite formatées suivant un format logique prédéterminé, et tout ou partie de ces informations sont encodées ou encryptées pour mieux les protéger selon le schéma défini par la table de sécurisation précitée. Il est à noter que ces opérations sont transparentes vis-à-vis des données et/ou applications à protéger.

Ensuite, les informations sont stockées sur un support d'enregistrement non réinscriptible qui est avantageusement à grande capacité de stockage et peu onéreux, comme par exemple un CDROM (disque optique numérique non effaçable) ou un DVD (vidéodisque numérique).

La deuxième phase concerne la sécurisation des plates-formes informatiques à partir desquelles les supports d'enregistrement pourront être utilisés et exploités en toute sécurité.

D'une manière générale, le procédé consiste à implémenter un dispositif matériel de sécurité avec au moins des mémoires du type ROM pour y enregistrer des logiciels de contrôle et de sécurité, et un contrôleur de gestion.

Il faut alors considérer deux cas, celui des plates-formes informatiques à architecture dite « fermée » et celui des plates-formes informatiques à architecture dite « ouverte ». Une plate-forme informatique est dite à architecture fermée lorsque cette

machine a été spécialement conçue ou adaptée pour mettre en oeuvre le procédé, c'est-à-dire qu'elle est déjà sécurisée en intégrant le dispositif matériel de sécurité et le logiciel associé. Par contre, une plate-forme à architecture dite ouverte n'est pas sécurisée pour mettre en oeuvre le procédé et, dans ce cas, il faut la sécuriser en implantant sous la forme d'une carte électronique le dispositif matériel de sécurité et le logiciel associé.

A ce stade, il faut noter qu'une solution de sécurisation uniquement logicielle est par définition fragile, et c'est pour cette raison que le procédé prévoit également la présence d'un dispositif matériel qui rend la sécurité plus fiable.

La fonction essentielle de ce dispositif matériel de sécurité et du logiciel associé, est d'interdire toute intrusion matérielle et/ou logicielle visant à accéder indûment au support d'enregistrement et aux informations stockées sur ce support ou à en faire usage en lieu et place d'un utilisateur autorisé et sans son accord, et de contrôler en permanence le déroulement du procédé dans les conditions de sécurité requises.

La troisième phase concerne l'accès et l'exploitation par un utilisateur potentiel d'un support d'enregistrement à partir d'une plate-forme informatique dûment sécurisée.

Pour illustrer cette troisième phase, on va expliciter un exemple dans lequel la première phase a été réalisée par un éditeur d'applications qui délivre gratuitement des supports d'enregistrement à des

utilisateurs, mais dont l'exploitation est payante selon des processus de facturation classiques.

Lorsque l'éditeur délivre un support d'enregistrement, il remet également à l'utilisateur un support portatif du type carte à puce par exemple.

Sur cette carte à puce, l'éditeur enregistre un certain nombre d'informations, comme par exemple et à titre non limitatif :

- un code d'identification propre à l'utilisateur ou PIN CODE, ce code n'étant toutefois pas imposé pour la mise en oeuvre du procédé,
- les clés de décodage ou de décryptage des informations stockées sur le support d'enregistrement,
- le niveau de sécurité requis pour exploiter les informations, et
- le paramètre d'identification propre aux données et/ou applications, qui correspond à celui enregistré sur le support.

Le support d'enregistrement et le support portatif vont être insérés dans des lecteurs appropriés qui équipent la plate-forme informatique sécurisée de l'utilisateur, et la mise en route générale de la plate-forme peut être effectuée.

Cette mise en route va être réalisée par un logiciel de contrôle qui est stocké dans le dispositif matériel de sécurité et qui va être exécuté pour piloter cette mise en route. A la mise sous tension, le dispositif matériel de sécurité s'initialise et va passer d'un état à un autre état sur la base de critères de temps. D'une manière générale, s'il ne reçoit pas des

informations ou un ordre dans un laps de temps déterminé, l'exécution du procédé est automatiquement arrêtée.

Dans un premier temps, le logiciel de contrôle va identifier le support d'enregistrement. Pour ce faire, le paramètre d'identification propre au support d'enregistrement est lu à partir du support et comparé avec celui qui a été préenregistré dans le dispositif matériel de sécurité. Ces deux paramètres sont vérifiés par le contrôleur de gestion, et s'ils ne sont pas identiques ou ne satisfont pas une relation prédéterminée, l'exécution du procédé est automatiquement arrêtée, le support d'enregistrement est inexploitable, la machine n'est plus sécurisée dans ce sens que le dispositif matériel de sécurité et le logiciel associé ne sont plus accessibles. Par contre, si la vérification est satisfaite, le support d'enregistrement a été correctement identifié mais cela ne suffit pas pour accéder et exploiter les données et/ou applications stockées, car le contenu du support a pu être modifié.

Dans un deuxième temps, le dispositif matériel de sécurité et le logiciel associé contrôlent l'intégrité du contenu du support d'enregistrement. A cet effet, la signature cryptée enregistrée sur le support est lue et le matériel de sécurité va la comparer avec une signature recalculée par lui-même ou par l'unité centrale de la plate-forme informatique à partir d'informations prélevées sur le support d'enregistrement, cette signature étant ensuite cryptée par le matériel de sécurité.

Si la comparaison de ces deux signatures cryptées ne donne pas un résultat satisfaisant, le matériel de sécurité en déduit que le contenu du support d'enregistrement a été modifié, c'est-à-dire qu'il n'est pas conforme à celui qui a été initialement produit. La mise en oeuvre du procédé est alors arrêtée, la plate-forme informatique n'est plus sécurisée et, de préférence, le fonctionnement de la plate-forme informatique est verrouillé. Autrement dit, l'utilisateur se trouve alors obligé de remettre en route la plate-forme informatique dans les conditions normales de fonctionnement mais avec impossibilité de pouvoir accéder et exploiter le support d'enregistrement, le dispositif matériel de sécurité et le logiciel associé devenant inaccessibles. Dans le cas contraire, le matériel de sécurité a reconnu l'intégrité du support d'enregistrement, c'est-à-dire que ce support est conforme à celui qui a été produit.

Dans un troisième temps, le matériel de sécurité vérifie le niveau de sécurité requis pour pouvoir exploiter les données et/ou applications du support d'enregistrement. A cet effet, le niveau de sécurité enregistré sur le support portatif de l'utilisateur est lu et comparé avec celui qui est enregistré sur le support. Si le niveau de sécurité n'est pas satisfait, la plate-forme informatique est verrouillée comme précédemment.

Dans un quatrième temps, le matériel de sécurité vérifie si l'utilisateur est autorisé à exploiter les données et/ou applications stockées sur le

support d'enregistrement. A cet effet, le dispositif matériel de sécurité lit le paramètre propre à l'application qui est enregistrée sur le support portatif de l'utilisateur et le compare avec le paramètre correspondant enregistré sur le support d'enregistrement. Cette comparaison peut se faire à l'identique ou suivant une relation prédéterminée. Si cette vérification ne donne pas un résultat satisfaisant, la plate-forme informatique est verrouillée comme précédemment.

Dans un cinquième temps, le dispositif matériel de sécurité vérifie que le logiciel de base de la plate-forme informatique n'a pas été éventuellement modifié pour détecter ainsi une éventuelle brèche dans la sécurité du procédé. Si une telle brèche est détectée, en utilisant des techniques connues, la plate-forme informatique est verrouillée comme précédemment.

Dans le cas contraire et dans une sixième temps, le dispositif matériel de sécurité et le logiciel associé vont brider le logiciel de base de la plate-forme informatique, notamment lorsque celle-ci est à architecture ouverte, c'est-à-dire que le dispositif matériel de sécurité va en quelque sorte mettre des verrous pour inhiber certaines fonctions du logiciel de base telles que celles qui pourraient normalement donner accès au support d'enregistrement, et mettre en place de nouvelles fonctions nécessaires au bon déroulement de l'exploitation des données et/ou applications à partir du support d'enregistrement, lorsque les contrôles effectués sur ce dernier et l'utilisateur ont été validés.

Avant d'entamer une seconde phase du processus d'amorçage, le dispositif matériel de sécurité et le logiciel associé vont installer, sous une forme standard et indépendante de l'implantation matérielle, une interface permettant d'accéder à l'intégralité des fonctions de sécurité qui seront notamment utilisées par le système d'exploitation lorsque ce dernier démarrera après avoir été chargé à partir du support d'enregistrement.

Jusqu'à maintenant, la première phase du processus de mise en route ou d'amorçage a permis de contrôler le support d'enregistrement et le droit d'accès de l'utilisateur, mais il faut maintenant qu'en retour des contrôles de sécurité soient effectués pour vérifier l'intégrité de la plate-forme informatique tant sur le plan matériel que logiciel.

A cet effet, un logiciel d'amorçage est chargé depuis le support d'enregistrement et est exécuté pour vérifier que les conditions de sécurité qui ont été satisfaites par le support d'enregistrement sous le contrôle de la plate-forme informatique, sont également satisfaites par la plate-forme informatique sous le contrôle du support d'enregistrement.

Ainsi, ce logiciel d'amorçage va notamment s'assurer :

- que le dispositif matériel de sécurité est bien implanté,

- que le logiciel de base de la plate-forme informatique a bien été bridé,

- que le paramètre d'identification propre au procédé et qui est enregistré dans le dispositif matériel de sécurité correspond bien à celui qui est enregistré sur le support d'enregistrement, et

- que le paramètre d'authentification du contenu du support d'enregistrement correspond à celui qui est également enregistré sur le support d'enregistrement.

Une fois tous ces contrôles effectués, on peut dire en quelque sorte que la plate-forme informatique est certaine d'accéder et d'exploiter un support d'enregistrement qui est conforme à celui qui a été produit et, inversement, le support d'enregistrement est certain d'être exploité par une plate-forme informatique dûment sécurisée et par un utilisateur dûment autorisé et dans la limite des droits qu'il a acquis.

Dans ces conditions, le chargement du système d'exploitation à partir du support d'enregistrement peut être envisagé. Cependant, comme le système d'exploitation est indépendant de celui de la plate-forme informatique, notamment lorsque cette dernière est d'une architecture « ouverte », il peut être nécessaire de faire appel à un logiciel de configuration qui est lu à partir du support d'enregistrement. La fonction générale de ce logiciel de configuration est de stocker dans le dispositif matériel de sécurité tous les paramètres nécessaires et suffisants pour que le logiciel d'exploitation des données et/ou applications et qui est stocké sur le support d'enregistrement puisse être exécuté par le logiciel d'exploitation de la plate-forme informatique.

Le logiciel d'exploitation peut donc être chargé à partir du support d'enregistrement pour permettre à l'utilisateur d'exploiter des données et/ou des applications en toute sécurité non seulement pour lui-même mais également pour l'éditeur des supports d'enregistrement.

Au cours de cette exploitation, la sécurité sera assurée par le logiciel d'exploitation qui a été chargé à partir du support d'enregistrement, ou par les applications elles-mêmes, et il s'appuiera pour cela sur l'interface précitée qui a été installée par le dispositif matériel de sécurité et le logiciel associé à la fin de la première phase du processus d'amorçage.

En effet, pour renforcer la sécurité du procédé, il est préférable que le système d'exploitation des données et/ou applications respecte aussi les fonctions de sécurité appliquées pendant la phase d'amorçage, comme par exemple interdire l'initialisation d'un logiciel non préalablement contrôlé ou l'accès à un périphérique non prévu par le procédé.

REVENDICATIONS

1. Procédé de sécurisation et de contrôle d'accès à des informations à partir d'une plate-forme informatique équipée d'un micro-ordinateur, caractérisé en ce qu'il consiste :

- à produire au moins un support d'enregistrement non réinscriptible sur lequel sont stockées des informations telles que des données et/ou applications selon un format logique prédéterminé, ainsi qu'un logiciel d'exploitation de ces informations,

- à définir les utilisateurs autorisés ayant un droit d'accès aux informations stockées sur ce support d'enregistrement et les limites éventuelles de ce droit d'accès,

- à configurer ou transformer la plate-forme informatique d'un utilisateur autorisé en un poste de travail sécurisé pour interdire toute intrusion matérielle et/ou logicielle visant à accéder indûment aux informations ou à en faire usage en lieu et place d'un utilisateur autorisé et sans son accord,

- à charger le logiciel d'exploitation à partir du support d'enregistrement qui est lu par un dispositif de lecture approprié de la plate-forme informatique,

- à permettre l'exploitation des informations stockées sur le support d'enregistrement dans les limites du droit acquis par l'utilisateur autorisé, et

- au cours de cette exploitation à échanger et/ou communiquer, de façon sécurisée, des données avec un réseau auquel la plate-forme informatique est reliée.

2. Procédé selon la revendication 1, caractérisé en ce que la phase de production d'un support d'enregistrement non réinscriptible consiste à définir les informations à protéger, le système d'exploitation de ces informations, un ensemble de paramètres de contrôle pour permettre le fonctionnement du logiciel d'exploitation chargé à partir du support d'enregistrement, et un ensemble de paramètres de sécurité pour sécuriser l'utilisation du support d'enregistrement d'une part, et l'exploitation des informations stockées sur ledit support.

3. Procédé selon la revendication 2, caractérisé en ce qu'il consiste à définir des paramètres de sécurité tels qu'un paramètre d'identification propre au procédé et un paramètre d'authentification du contenu du support d'enregistrement sous la forme d'une signature cryptée, pour sécuriser l'utilisation dudit support.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce qu'il consiste à définir des paramètres de sécurité tels qu'un paramètre concernant un niveau de sécurité requis et un paramètre propre aux données et/ou applications, pour pouvoir exploiter le support d'enregistrement.

5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce qu'il consiste à coder ou encrypter tout ou partie des informations, et à stocker également sur le support d'enregistrement une table de sécurisation contenant les algorithmes de décodage sous une forme cryptée.

6. Procédé selon l'une quelconque des revendications 2 à 5, caractérisé en ce que la phase de configuration ou de transformation d'une plate-forme informatique en un poste de travail sécurisé consiste à implémenter dans ladite plate-forme un dispositif matériel de sécurité et un logiciel associé, pour interdire toute intrusion matériellle et/ou logicielle pour mettre en oeuvre des fonctions de sécurité à partir des paramètres précités.

7. Procédé selon la revendication 6, caractérisé en ce qu'il consiste à associer au dispositif matériel de sécurité un support portatif, tel qu'une carte à puce, sur lequel sont enregistrées des informations concernant les droits concédés à chaque utilisateur potentiel.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste, avant de charger le logiciel d'exploitation à partir du support d'enregistrement, à faire exécuter des fonctions de sécurité par le dispositif matériel de sécurité pour vérifier que le support d'enregistrement est bien conforme à celui qui a été produit, et à vérifier, à partir d'un logiciel d'amorçage chargé depuis le support d'enregistrement, que les conditions de sécurité qui ont été satisfaites par ledit support sous le contrôle de la plate-forme informatique, sont également satisfaites par cette dernière sous le contrôle dudit support.

9. Procédé selon la revendication 8, caractérisé en ce qu'il consiste à rendre indépendant le

système d'exploitation stocké sur le support d'enregistrement et celui de la plate-forme informatique, et à charger si nécessaire un logiciel de configuration à partir dudit support pour fournir les paramètres nécessaires à l'exécution du système d'exploitation stocké sur ledit support.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste, après chargement du système d'exploitation à partir du disque d'enregistrement, à faire exécuter par ledit système des fonctions de sécurité tant vis-à-vis du support d'enregistrement que de la plate-forme informatique, pour renforcer la sécurité de la mise en oeuvre du procédé.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2756074
N° d'enregistrement national

FA 535243
FR 9613951

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, vol. 37, no. 11, 1 Novembre 1994, pages 66-70, 94, XP000485634 "BITS: A SMARTCARD PROTECTED OPERATING SYSTEM" * page 68, colonne de gauche, alinéa 2 - colonne de droite, alinéa 1 *	1,2,4,6,7
A	---	3,8
Y	EP 0 421 409 A (IBM) 10 Avril 1991 * abrégé; figures 4,8,11,15 * * page 1, ligne 18 - page 4, ligne 18 * * page 7, ligne 28 - ligne 37 * * page 8, ligne 41 - page 12, ligne 52 * * page 11, ligne 27 - ligne 45 *	1,2,4,6,7
A	---	5,9
A	WO 95 24696 A (INTEGRATED TECH AMERICA ;MOONEY DAVID M (US); KIMLINGER JOSEPH A () 14 Septembre 1995 * revendications 1-20 *	1,4-6,8
A	--- US 5 191 611 A (LANG GERALD S) 2 Mars 1993	
A	--- US 5 444 850 A (CHANG STEVE M) 22 Août 1995	
A	--- EP 0 737 907 A (SECURE COMPUTING CORP) 16 Octobre 1996	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
G06F

Date d'achèvement de la recherche	Examinateur
21 Août 1997	Powell, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1